TRANSCRIPT

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

East Melbourne – Thursday 26 September 2024

(via videoconference)

MEMBERS

Alison Marchant – Chair

Kim O'Keeffe – Deputy Chair

Anthony Cianflone

Wayne Farnham

John Mullahy

Dylan Wight

Jess Wilson

WITNESS

Dr Fiona Macdonald, Policy Director, Industrial and Social, Centre for Future Work, Australia Institute.

The CHAIR: Welcome to the public hearing for the Legislative Assembly Economy and Infrastructure Committee's Inquiry into workplace surveillance. All mobile telephones should now be turned to silent.

All evidence given today is being recorded by Hansard and broadcast live on the Parliament's website.

While all evidence taken by the Committee is protected by parliamentary privilege, comments repeated outside of this hearing, including on social media, may not be protected by this privilege.

Witnesses will be provided with a proof version of the transcript to check. Verified transcripts and other documents provided to the Committee during the hearing will be published on the Committee's website.

I just remind members and witnesses to mute their microphones when not speaking, to minimise interference.

Thank you so much, Dr Fiona Macdonald, for joining us today, and thank you for your submission to the to the Committee. We thought we might allow you a few minutes to either talk to your submission or add anything further you would like to start us off on a discussion today, and then I will get the Committee members maybe to ask you some further questions as well. I will hand over to you.

Fiona MACDONALD: Thank you, Chair. Thank you for inviting us to make a submission and me to be here today. I am representing the Centre for Future Work. We are a centre that conducts labour market work and employment research. We are situated within the Australia Institute, which is an independent policy and research think tank. Our centre has been conducting research into a broad range of workplace issues—our centre and our researchers—over many, many years. The centre in particular, since its inception in 2016, has taken a particular interest in the implementation and use of technologies in the workplace, and we draw on that work, in addition to some policy reports that we have noted in our submission. We also draw on current work that we are undertaking involving an intense, extensive review of international literature on these issues.

I will not spend a lot of time talking to our submission, other than to say that we believe it is a critical time to act to address what we see as some serious risks associated with the ongoing intensive surveillance and monitoring that is being undertaken in workplaces that changes. While it can be seen as a continuation of the kinds of surveillance and monitoring that employers have always engaged in in relation to employees' performance, it has some significant qualitative differences, including the way that data is connected to AI applications at work, which has some serious implications, and also the intensity and extent of monitoring and surveillance, which has now gone well beyond the boundaries of the workplace, work time and legitimate work activities. Thank you. I will stop there for the moment.

The CHAIR: Thank you for that. We will unpick some of that in questions to you. Can I just confirm that there was a study? You said you did a national study in 2018 and you were talking about the percentage of workers that said that their employer had used one or more forms of surveillance, and some of that was monitored outside of their workplace as well.

Fiona MACDONALD: Yes.

The CHAIR: Do you know or do you have any evidence around what happened post COVID?

Fiona MACDONALD: Post COVID we have not conducted that survey again. Our assessment of what has happened post COVID is based on our monitoring of anecdotal reports but also our understanding of what is happening overseas and in the international literature. The other important factor in terms of understanding what is happening now is actually found in the data that is very publicly available in relation to what, say, for example, software companies are doing, who their clients are and how extensive their engagement is. For example, Workday, which is very frequently connected up to Microsoft computer systems, advertise that they have a very large number of very large employers as their partners or clients in Australia, and those software systems they advertise—it is publicly available what those software systems do. They collect masses of amounts of data, and that data is used to feed into performance management systems which are also connected to external datasets and are used through predictive analytics to predict what employees may do. That is just one example of one of the—I was going to go on and talk about the risks of that, but I think I just really, in answering your question, wanted to say that it is very apparent from the software that is out there and the extent to which that is being used in organisations in Australia—that tells us a lot about the extent of surveillance.

The CHAIR: And that blurring of the line between workplace and home and still being surveilled outside of the work hours and some workers not understanding the full extent of the surveillance that has been happening.

Fiona MACDONALD: And again, another example is for an area that I have done a lot of work in, which is with home care workers. Those workers now, their interactions with their organisation are through their mobile phones, and their mobile phones track them. They track their conversations that are used via those apps. They track conversations they may have via those apps with other workers, so there is a real blurring of home and work and there are no clear boundaries that are transparent to employees and workers around that. Again, cameras in vehicles are now used a lot for safety, but they are also monitoring conversations undertaken at any time in those vehicles. So those boundaries are really not apparent always to employees, and they are crossed all the time, given the reliance on those technologies in everything we do and for everything we do.

The CHAIR: Yes. Thank you for that. I will go to some other committee members to ask some questions. Wayne, I will go to you first.

Wayne FARNHAM: Thank you, Chair. Thank you for your submission, Dr Macdonald, and for coming here today. Just following on from the Chair, it was interesting reading about your 2018 survey. I think the part that concerned me in that was that 18 per cent were digitally monitored outside their workplace. I think that is pretty wrong. Now, the federal government has just passed laws about contacting employees out of hours of work, so after 5 o'clock at night the employer cannot contact the employee. Do you think they should have gone further with that and included surveillance in that?

Fiona MACDONALD: That is a good question. I had not thought of that, but I think that that legislation specifically was responding to a concern about work interruptions outside people's work hours. So it was not actually even responding to, for example, a manager might access a person's file outside their work hours to answer a question the manager wants answered outside work hours, which could be seen in some way as contact outside work hours. But that right-to-disconnect legislation is specifically around interrupting home time and creating unpaid overtime. I think that is the real intention of that legislation, so stopping that unpaid overtime, that creeping availability to your employer that occurs for many workers with that ability to be contacted all the time. So potentially that legislation could have done that, but I think it has a very different purpose.

Wayne FARNHAM: Do you think, Dr Macdonald, that there should be legislation introduced that does address the surveillance of workers outside of work hours?

Fiona MACDONALD: I do. I believe in dealing with the changes that we need to privacy legislation and/or through the proposed federal government's AI guardrails there is one mechanism through which that could be done. That proposal is to take a risk management approach. I think that that approach still requires some forms of contact to be prohibited and some forms of surveillance to be prohibited and monitoring to be prohibited. Among those prohibitions should be a prohibition on monitoring surveillance outside of work.

Wayne FARNHAM: Sorry, Chair, just one last one here. We seem to have a state-by-state approach to this—like, New South Wales and ACT have already got laws introduced. Do you think a national approach would be better, where all the states are harmonised with the same law so we do not have different cross-border laws? For example, you might live in Wodonga and work in Albury and you have those crossed laws. Do you think a national approach to this would be a better way to ensure workplace safety around workplace surveillance and breaches of privacy? Do you think that would be a better model, or state by state?

Fiona MACDONALD: I do think a national approach would be the best model. If we look at the government's AI guardrails proposals, they are looking at three options. One of those options is to provide a framework that would still require changes to existing legislation. Its requirements would be enacted through changes to current state laws rather than bringing in a whole new AI Act that would potentially cover these issues itself. One of the options would still be to achieve the changes through changes to state laws. While it would be in an ideal world for the problems to be addressed nationally, I think we have to start with where we are at and address the changes through current state legislation because there are too many unknowns in terms of where and how federal legislation might impact on state legislation in the future.

Wayne FARNHAM: Thank you, Dr Macdonald. I have been a bit greedy. I will let some of my other colleagues have a question. Thank you.

The CHAIR: That is completely fine. They were good questions, Wayne. I will go to you, Anthony.

Anthony CIANFLONE: Thanks also, Dr Macdonald, for appearing and for the submission from the institute. Going through your submission you do highlight and talk about how workplace surveillance practices have become more intensive and more pervasive. Picking up on what Wayne was saying, particularly that 18 per cent research point around outside-hours monitoring is very concerning, and dare I say that may have potentially very much increased post COVID given they were pre-COVID figures. Does the Australia Institute have any examples around how these practices impact on the health and wellbeing of workers, whether it is during work hours and particularly outside work hours? Do you have any examples or case studies potentially you could talk to or point to?

Fiona MACDONALD: We do have the data that we collected in that 2018 survey in which workers spoke about the stress and anxiety created. I think there is an enormous amount of anecdotal data to that in Australia—performance pressures that are created through intensive monitoring. There is also really good international research that takes the example of electronic monitoring of customer service officers, where we see how extensive and pervasive monitoring creates enormous performance pressures, can lead to physical strain injuries and leads to people cutting corners in safety procedures to try to keep up with what the considered performance expectations are. I can direct you to some of that research. Some of it was cited in the submission that we lodged with the federal government inquiry. That is referenced at the back of our submission. Then there is also the unfairness in the surveillance, its impact on people's rights to procedural fairness and the removal of the human element. It is that old management adage: you manage what you can measure. When you are using partial measurements that are collected by data monitoring and AI systems and those become your performance measures, they are partial measures. Removal of human judgement in those instances can lead to quite unfair decisions. Similarly, the use of monitoring of workers' availability that is fed into rostering systems can also lead to those kinds of problems.

Anthony CIANFLONE: We had a witness earlier on—I am not sure if you Zoomed in or were tuning into it by any chance—a very credible, well-researched, very strong background witness, who has done some phenomenal work in the neuroscience space, neurotechnology. They were very much talking to what the future may potentially look like with the introduction of neurotechnology literally in workers' brains or in the physical realm of workers to detect and monitor, for one part of what was being discussed, a worker's performance or mood or emotions or have the potential to intervene at certain points for OHS and safety reasons. What is the Australia Institute's view about that sort of technology being floated and potentially introduced on top of what is already in place down the track?

Fiona MACDONALD: That kind of technology we need to understand the risks of and we need to be aware of those. We already know that the nudges that are used to change workers' behaviour, the use of technology to monitor and manage workers' behaviour—the monitoring systems measure emotions through measuring tone in voice and through facial expressions. On the one hand there are the risks associated with that through the stress, anxiety and performance pressures placed on employees, but the other risks are the ways in which that data is then used in AI systems and fed in to change individual behaviour, push individuals to behave in certain ways and manipulate them but also the ways in which that data is fed into larger predictive analytic systems that draw on a whole heap of outside data and a whole heap of psychological study findings to profile basically individuals and make predictions about (a) their likelihood of staying in an organisation or (b) their likelihood of becoming a leader. Workers' futures will be determined on the basis of those kinds of analyses. Nobody has any idea how fair that is, and there is good evidence that it is not.

Anthony CIANFLONE: So the Australia Institute is not advocating for neurotechnology to be introduced into workplaces.

Fiona MACDONALD: No, we are not. Sorry, that should have been my short answer.

Anthony CIANFLONE: They are my questions.

The CHAIR: Thank you, Anthony. I will go to you, John.

John MULLAHY: Thanks, Chair; and thanks, Dr Macdonald, for being here today and your submission. We have had quite a bit of evidence with regard to the issue around employer transparency, and I just want to

get an idea of the Centre for Future Work's ideas around what information employers should be required to provide workers about workplace surveillance, the use of AI and associated data.

Fiona MACDONALD: I think we need to shift the way that we think about that and actually establish a preventative approach. We need to put some prohibitions around what workers can monitor, as we have talked about, in terms of outside hours and collection of personal data where that is unnecessary. The starting point needs to be building systems of privacy regulation around workplace monitoring and surveillance that start from the point of view of accountability. Employees need to know what data is being collected, if there is a good reason for collecting it, how it is being collected and how it will be stored. Rather than this happening after the fact, a preventative approach starts from the basis of accountability for all of that, so the intention to collect particular data and transparency around what it is and what is done with it needs to be at the outset before it is implemented. So you need regulation that supports consultation prior to rather than after-the-fact redress or addressing violations—it needs to be set up at the beginning. I think again it is very difficult for employers to be knowledgeable about how some of the data is used, so if employers are not able to be clear on how data that they are collecting is used, then they should not be able to collect it.

John MULLAHY: Sorry. I was interested—there would be consultation with employees, so therefore the employer knows and the employee knows exactly what data is being collected, but what would you suggest with regard to the access that employees should have to that data?

Fiona MACDONALD: The access employees should have to that data I think would depend on what the data is. If decisions are being made on the basis of data, then employees should know what that data is. Where data is used to impact on employees, employees should have access to that data.

John MULLAHY: Thanks, Fiona.

The CHAIR: Thanks, John. Dylan, I will head to you next.

Dylan WIGHT: Thank you, Chair. Thank you for your evidence as well. We have heard evidence throughout this inquiry, particularly from unions, about instances of companies using surveillance to essentially stop workers organising, sometimes blocking union emails coming in or emails going out to unions et cetera. What steps can the Victorian Government take to protect workers' explicit right to organise collectively?

Fiona MACDONALD: That is a tricky one, because those rights sit within the Fair Work Act, which does not actually support workers organising around these matters. Adverse action is addressed within the Fair Work Act, but employees have to know that that action has been taken, and also they need to know what data has been collected and how it has been collected. In terms of action that the Victorian Government can take, that would be in a privacy Act in strengthening the accountability of employers around the data they collect and how they collect it. I do not have any suggestions for specific ways in which you might deal with that issue.

Dylan WIGHT: A road you are going down we have heard a fair bit of evidence on as well is around giving employees access to the data that is collected on them. So if there is a situation where an employer is interfering with an employee's right to collectively organise, they would have access to that and then through the Fair Work Act they can use the adverse action provisions or general protection provisions to go to the Fair Work Commission and prosecute it.

Fiona MACDONALD: It is understanding what data is collected and employers being accountable for not just what they collect but why they collect it and whether it is necessary to collect it, so some boundaries being put around what is collected. There has to be a reasonable use of that data, and if there is a privacy issue, it has to be balanced. So at the outset there have to be discussions about what data is collected and what is done with it, not just leaving it to employees to assess how that data is being used once they know what it is—a preventative approach.

Dylan WIGHT: Yes. Thank you.

The CHAIR: Thank you. I think we have probably got time for another question. I am going to ask that if that it is okay, Fiona, about AI. This committee has heard about how the increased use of AI is really unknown—where it will go and what it will do—and also in relation to companies using technology that they thought was doing one function but then they find that the functionality can creep into other areas and it does a

whole lot of other things when AI is also introduced. Do you have a view on measures or things that we should do in Victoria that require software or AI manufacturers to comply with certain regulation? Do you have a sense of what that could look like?

Fiona MACDONALD: No, I do not. I think I would look at it through the lens of the federal legislation, which aims to set guardrails around all developers and deployers of software and the need for them to make clear what their software does, where data goes, how it can be used. If there is potential for the state to act through any existing or new legislation to strengthen that, I think that that would be a good thing despite the ideal world where we might have it all managed federally; I do not think that that is realistic.

The CHAIR: On that, though, if the federal legislation does not go particularly heavily in the workplace sense and just does general AI, do you suggest that Victoria has something in legislation around AI and the use of AI?

Fiona MACDONALD: Yes. Victoria could well have surveillance and AI specific legislation. It does appear from the way that the federal government is approaching things that the workplace keeps falling to the bottom of the list of priorities in terms of the specific workplace issues being addressed, and it also appears that it may be a long time until that focus is really tightened and the understanding of what is happening in the workplace is really fed into any federal proposals, I believe—or I fear.

The CHAIR: Yes. Thank you so much for your time today, your submission and helping us with some questions. We really appreciate it. It gives us lots of food for thought.

Fiona MACDONALD: I really appreciate the opportunity, and I wish you all the best with your endeavours.

The CHAIR: Thank you so much.

Witness withdrew.